公告本

91年3月04日 修正補充

申請日期	90.04.10
案號	90106611
類別	H04L12/56, H04L29/00

（以上各欄由本局填註）

A4
C4

484282

發明 新型 專利說明書

修正本 91.2.4

一、發明新型名稱	中文	網路交換系統對線上封包之監控管理方法
	英文	
二、發明創作人	姓名	官炳松
	國籍	中華民國
	住、居所	新竹科學工業園區園區二路20號
三、申請人	姓名（名稱）	友訊科技股份有限公司
	國籍	中華民國
	住、居所（事務所）	新竹科學工業園區園區二路20號
	代表人姓名	高次軒

經濟部智慧財產局員工消費合作社印製

本紙張尺度適用中國國家標準（CNS）A4規格（210×297公釐）

裝 訂 線

五、發明說明（1）

發明背景：

本發明係一種網路交換系統(Switching System)對線上封包之監控管理方法，尤指一種可令一網路交換系統能根據使用者設定，對所欲進行監控之節點傳來之封包資料，依使用者於一轉送設定表內各欄位中所設定之參數值，進行即時學習、擷取、收集、監控及轉送處理之方法。

先前技術：

按，目前在乙太網路(Ethernet)上，參閱第 1 圖所示，不同區段之乙太網路 11、12、13、14 均係藉與一個以上之網路交換器 30(switch) 相連接，參閱第 1 圖所示，該交換器 30 可爲一具有複數個連接埠(port)之網路裝置，無論其外觀係由複數個網路裝置堆疊而成或僅係單一之網路裝置，只要該等交換器間係藉相同之橋接協定封包(Bridge Protocol Data Units，簡稱 BPDUs)，進行彼此溝通，均爲本發明所稱之網路交換系統。

一般言，該等傳統網路交換器 30 均係透過其上所安裝之控制器或軟體，對傳送至該網路交換器 30 之所有封包資料之來源位址及目的位址進行學習，並藉由建立或更新其上所設之一轉送對應表(Forwarding Table)，做爲封包資料轉送(Forwarding)之依據，將所接收之封包資料轉送至該轉送對應表中記錄之目的位址 (Destination)之連接埠。意即，當該等交換系統 30 之連接埠(port)1、2、3、4

五、發明說明（2）

分別接收到由各區段網路(Segment) 11、12、13、14 上之節點(Node) A、B、C、D 傳來之封包資料時，該等交換系統 30 能針對該等封包資料之目的位址及來源位址，至該轉送對應表(Forwarding Table)31 中，參閱第 2 圖所示，與其已記錄之位址進行下列比對及處理：

(1) 若發現該封包之來源位址不存在於該轉送對應表 31 時，該交換系統 30 即將該封包之來源位址及其連接埠記錄於該轉送對應表 31 中，以完成對該封包來源位址之動態登錄；

(2) 若發現該封包之來源位址已存在於該轉送對應表 31 時，該交換系統 30 即更新(update)該轉送對應表 31 中已記錄之來源位址之連接埠欄位，完成對該封包連接埠之動態更新；

(3) 若發現該封包之目的位址係屬同一區段網路之節點，該交換系統 30 即丟棄該封包，而不作任何傳送，以完成對封包傳送之過濾(filtering) ；

(4) 若發現該封包之目的位址已存在於該轉送對應表 31 時，該交換系統 30 即將該封包傳送至該目地位址之連接埠，完成對該封包之即時轉送；

(5) 若發現該封包之目的位址不存在於該轉送對應表 31 時，該交換系統 30 即將該位址氾送(flooding)至每一個正在使用中之連接埠，若目的位址之節點對該封包回應，該交換系統 3 即將該目的位址記錄於該轉送對應表 31 中，以完成對該封包來源位址之動態登錄。

五、發明說明（3）

該網路交換系統即藉此種學習功能，維持該轉送對應表 **31** 之完整性及正確性，且依該轉送對應表 **31** 內之資訊，對網路上之各節點，提供網路連繫所需之資料，故，一旦俟所有節點都被學習後，封包一進入該網路交換系統 **30** 時，即可依據該轉送對應表所記錄之資料，直接將封包轉送到目的位址之節點。然而，由於現今網路交換系統之連接埠數目愈來愈多，其轉送對應表亦隨之愈來愈大，此一現象，對於系統資訊管理(Management Information System，簡稱 MIS)人員而言，不僅建立一可安全控制之轉送對應表，已成爲一冗長又容易出錯之工作，且由於該項學習**(learning)**之功能，亦令管理人員無法輕易將該轉送對應表，予以鎖定(locking)，致未經授權之節點之來源位址得任意佔用該轉送對應表之記憶空間，且該種傳統網路交換系統對網路駭客**(hacker)**之試探性上線，亦因其具備逾時資訊自動刪除之計時(auto aging out timer)功能，而無法有效掌握其資訊源頭，造成網路安全機制上之嚴重問題。

另，由於傳統網路交換系統中所運用之前述封包學習及轉送技術，令網路交換系統對封包之收集及監控處理，僅能在該等網路交換系統之外部，透過 **Shiffer** 或 **mirror** 之方式，對單一連接埠進行封包之收集及監控，或由該等網路交換控制器提供一計數器，對封包流量**(traffic utilization)** 及大小進行監控，故傳統網路交換系統並無法對不同網路區段間所傳來之封包資料，尤其是特定節點之封包資料，進行有效之監控處理，以確實掌握特定節點之動向。

五、發明說明（4）

此外，由於網路交換系統產品在研發階段，常需藉其它設備，如：集線器(Hub)、Shiffer 或 PC 等設備，對線上封包進行收集及分析處理，其過程不僅煩鎖耗時，且產品在實驗室驗證階段，當問題發生時，亦無法做立即有效之分析處理。

發明綱要：

有鑒於前述傳統網路交換系統無法直接對不同網路區段間所傳來之封包資料，進行有效監控處理，以確實掌握特定節點動向之問題，發明人乃研究出一種網路交換系統之線上封包之監控管理方法，期令本發明之網路交換系統，能根據使用者設定，依其上原有之一轉送對應表(Forwarding Table)進行修改，並建立一轉送設定表(Forwarding Configuration Table)，俾經過該網路交換系統之封包資料，能先被轉送(Forwarding)到該網路交換系統之一中央處理器(CPU)，再利用該中央處理器(CPU) 對所欲進行監控之節點傳來之封包資料，依使用者於該轉送設定表內各欄位中所設定之參數值，進行即時擷取、收集、監控及轉送處理。

本發明之一目的，係令該網路交換系統不僅可令保有原先之學習及轉送功能，且可直接對不同網路區段間所傳來之封包資料，進行有效監控處理，以確實掌握特定節點之動向。

本發明之另一目的，係令使用者可藉本發明之方法，對網路上所發生之異常(如：擴展樹(Spanning Tree)一直做(Topology Chain)或控制封包(control frame)

五、發明說明（5）

送收異常)或其它未經許可之不正常存取現象（如：駭客入侵或單純之侵入等），鎖定特定之節點，對所傳來之封包資料，進行即時擷取、收集或問題之分析及監控處理，以有效提昇網路之安全保障。

今，爲能更清楚地表達本發明之技術手段及運作過程，茲配合附圖舉一較佳實施例，說明如下：

附圖說明：

第 1 圖所示乃乙太網路與一般網路交換系統間之連線示意圖；

第 2 圖所示乃一般網路交換系統之轉送對應表之示意圖；

第 3 圖所示乃本發明之網路交換系統之示意圖；

第 4 圖所示乃本發明之網路交換系統之轉送設定表之示意圖；

第 5 圖所示乃本發明之一實施例對指定節點進行監控前之流程示意圖；

第 6 圖所示乃本發明之一實施例之轉送對應表之示意圖；

第 7 圖所示乃本發明之一實施例之轉送設定表之示意圖；

第 8 圖所示乃本發明之一實施例之網路交換系統對指定節點進行線上封包監控處理之流程示意圖。

主要元件符號說明：

五、發明說明（6）

網路交換系統……40　　轉送對應表……42

轉送設定表……43　　中央處理器……41

連接埠……1、2、3、4　　區段網路……11、、12、13、14

節點……A、B、C、D

詳細說明：

本發明係一種網路交換系統(Switch)之線上封包之監控管理方法，該方法主要係令一網路交換系統 40 能根據使用者設定，參閱第 3 圖所示，依其上原有之一轉送對應表(Forwarding Table)42，建立一轉送設定表(Forwarding Configuration Table)43，俾經過該網路交換系統 40 之封包資料，能先被轉送(Forwarding)到該網路交換系統之一中央處理器(CPU)41，再利用該中央處理器 41 對所欲進行監控之節點 A、C 傳來之封包資料，依使用者於該轉送設定表內各欄位中所設定之參數值，進行即時擷取、收集、監控及轉送處理。

在本發明之一最佳實施例中，該轉送設定表 43 至少包括如下欄位，參閱第 4 圖所示：

(1)節點(Node)欄位：係用以存放使用者欲進行監控之各節點，即來源位址。

(2)連接埠(Port)欄位：係用以存放各該被監控節點所對應之連接埠。

(3)擷取連接埠(Capture Port)欄位：係用以存放進行擷取時之目的連接埠或

五、發明說明（7）

使用區域緩衝器，俾利用該等擷取連接埠，分別擷取由對應區段網路(Segment) 11 或 13 上各節點(Node) A 或 C 透過各該被監控連接埠傳來之封包資料。

(4)狀態(State)欄位：係針對該節點(Node)欄位中所設定之各節點，存放收集封包時之狀態參數，以決定收集方式，該狀態參數依其對該被監控之節點所傳來之封包資料，是否進行收集或過濾，可分爲至少下列幾種方式：

a) 不收集，且不過濾；

b) 不收集，但要過濾；

c) 收集，但不過濾；

d) 收集，且要過濾；

e) 不啓動對節點之監控。

(5)觸發(Trap)欄位：係針對該節點(Node)之連接埠變更時，存放是否要觸發該網路交換系統 40，或透過其上之使用者介面，通知使用者此一變動之參數。

在本發明之該實施例中，該交換系統 40 對網路上傳來之所有封包具有學習及轉送之功能，故該交換系統 40 之各連接埠 1、2、3、4 在接收到各區段網路 11、、12、13、14 之節點 A、B、C、D 所傳來之封包資料時，該等交換系統 40 之中央處理器 41 可針對該封包之目的及來源位址，至該轉送對應表 42，與其已記錄之位址進行比對，並完成對該封包來源位址及目地位址之動態登錄、更新及過濾處理，以維持該轉送對應表之完整性及正確性，且依該轉送對應表 42 內之資訊，對

五、發明說明（8）

網路上之各節點，提供網路連繫所需之資料，並依該轉送對應表所記錄之資料，直接將封包轉送到目的位址。

當使用者欲對該網路交換系統 **40** 上由某一節點 **A** 所傳來之封包資料，進行監控處理時，該使用者可透過一網路終端主機，輸入該節點參數，再將其下載(download)至該網路交換系統，或直接由使用者透過網路管理程式，設定該節點參數。此時，參閱第 **6** 圖所示，該網路交換系統 **40** 立即修改該轉送對應表 **42** 內之記錄，將其上節點欄位 **A** 所對應之連接埠欄位，修改爲與該網路交換系統 **40** 之中央處理器**(CPU)41** 連線埠狀態，參閱第 **6** 圖所示，俟該節點 **A** 被設定爲監控之對象後，該中央處理器 **41** 立即依該轉送對應表 **42** 建立一轉送設定表 **43**，參閱第 **7** 圖所示，俾該中央處理器 **41** 在偵測到流經該網路交換系統 **40** 上之封包資料之來源位址或目的位址係節點 **A** 時，立即依該轉送設定表 **43** 內使用者所設定之其它參數值，進行下列監控及轉送處理，參閱第 **8** 圖所示：

(1)首先，由所接收之封包資料中，判斷節點 **A** 之連接埠是否有變更，若有變更，即針對該轉送設定表 **43** 中原對應至該節點之連接埠參數，進行更新**(update)**，並判斷該轉送設定表 **43** 內之觸發**(Trap)**欄位，是否設定有觸發參數，若設定有觸發參數，即透過其上之使用者介面，通知使用者此一變動情事；否則，繼續下列步驟；

(2)判斷該轉送設定表 **43** 中擷取連接埠欄位內所設定之連接埠參數 **5**，俾將

五、發明說明（9）

所接收之封包資料，轉送至該連接埠 5 並由所連接之裝置 E 擷取下來，參閱第 3 圖所示，以對所擷取之封包資料進行其它分析及監控處理；否則，繼續下列步驟；

(3)判斷該轉送設定表 43 中狀態欄位內所設定之參數值，俾依該參數對所接收之封包資料，進行過濾或收集處理，並於完成該等處理後，依該轉送設定表 43 中連接埠欄位內所設定之連接埠參數，將封包轉送到該網路交換系統 40 上之該連接埠，並透過該連接埠將封包轉送到其目的位址。

利用本發明之方法，當未經授權之特定節點進入該網路交換系統時，該網路交換系統可立即根據其連接埠之異動狀態，觸發網管或使用者介面，即時向網路管理人員發出警告，且可令該網路管理人員據此分析是否有網路駭客(**hacker**)盜用該節點，或將該節點移至其它網路區段，直接對不同網路區段間所傳來之封包資料，進行有效之監控處理，以確實掌握特定節點之動向，有效提昇網路之安全機制。此外，對於研發階段之網路交換系統，亦可在發生問題時，藉鎖定特定之節點，對所傳送之封包資料，進行擷取及收集，以進行即時監控及分析處理，迅速找出問題徵結，並予妥善處理。

按，以上所述，僅爲本發明最佳之具體實施例，惟本發明之構造特徵並不侷限於此，任何熟悉該項技藝者在本發明領域內，可輕易思及之變化或修飾，皆可涵蓋在以下本發明之專利範圍內。

A5
B5

四、中文發明摘要（發明之名稱：網路交換系統對線上封包之監控管理方法）

本發明係一種網路交換系統(Switching System)對線上封包之監控管理方法，該方法主要係令一網路交換系統能根據使用者設定，依其上原有之一轉送對應表(Forwarding Table)進行修改，並建立一轉送設定表(Forwarding Configuration Table)，俾經過該網路交換系統之封包資料，能先被轉送(Forwarding)到該網路交換系統之一中央處理器(CPU)，再利用該中央處理器對所欲進行監控之節點傳來之封包資料，依使用者於該轉送設定表內各欄位中所設定之參數值，進行即時學習、擷取、收集、監控及轉送處理。

英文發明摘要（發明之名稱：）

A8
B8
C8
D8

六、申請專利範圍

1.一種網路交換系統對線上封包之監控管理方法，該方法主要係令一網路交換系統根據使用者之設定，修改其上所設之一轉送對應表內至少一被監控之節點所對應之連接埠欄位值，令該被監控之節點變成與該網路交換系統之一中央處理器相連線之狀態，並建立一轉送設定表，俾該中央處理器依該轉送設定表中一節點欄位所對應之各欄位內之設定參數值，對該被監控節點傳來之封包資料，進行擷取及監控處理，並於完成該等處理後，再依該轉送設定表內該被監控節點所對應之一連接埠欄位值，將封包資料透過該連接埠轉送到其目的位址。

2.如申請專利範圍第 1 項所述之一種網路交換系統對線上封包之監控管理方法，其中該轉送設定表尚包括一觸發欄位，係用以存放當該被監控節點變更其連接埠時，是否要觸發該網路交換系統之參數，以透過一使用者介面，通知使用者此一異動情形。

3.如申請專利範圍第 2 項所述之一種網路交換系統對線上封包之監控管理方法，其中該中央處理器在偵測到流經該網路交換系統之封包資料之來源位址或目的位址係該被監控之節點時，將立即依該轉送設定表內使用者所設定之參數值，進行下列監控及轉送處理：

判斷該被監控節點之連接埠是否變更，若是，立即更新該轉送設定表中之連接埠，並判斷該轉送設定表內之該觸發欄位，是否有觸發參數，若是，即透過一使用者介面，通知使用者此一異動情形，並於完成該等處理後，依該轉送設定表

六、申請專利範圍

中該連接埠欄位內所設定之連接埠，將封包資料透過該連接埠轉送到其目的位址。

4.如申請專利範圍第 1 項所述之一種網路交換系統對線上封包之監控管理方法，其中該轉送設定表尚包括一擷取連接埠欄位，係用以存放使用者所指定之一擷取連接埠，俾利用該擷取連接埠，擷取由該被監控節點所對應之連接埠傳來之封包資料。

5.如申請專利範圍第 4 項所述之一種網路交換系統對線上封包之監控管理方法，其中該中央處理器在偵測到流經該網路交換系統之封包資料之來源位址或目的位址係該被監控之節點時，將立即依該轉送設定表內使用者所設定之參數值，進行下列監控及轉送處理：

判斷該轉送設定表中該擷取連接埠欄位內所設定之連接埠參數，俾將所接收之封包資料，由該連接埠所連接之裝置擷取下來，進行分析及監控處理，並於完成該等處理後，依該轉送設定表中該連接埠欄位內所設定之連接埠，將封包資料透過該連接埠轉送到其目的位址。

6.如申請專利範圍第 1 項所述之一種網路交換系統對線上封包之監控管理方法，其中該轉送設定表尚包括一狀態欄位，係用以存放自該被監控節點收集封包時之狀態參數，以根據該狀態參數判斷是否對該被監控節點傳來之封包資料，進行收集或過濾。

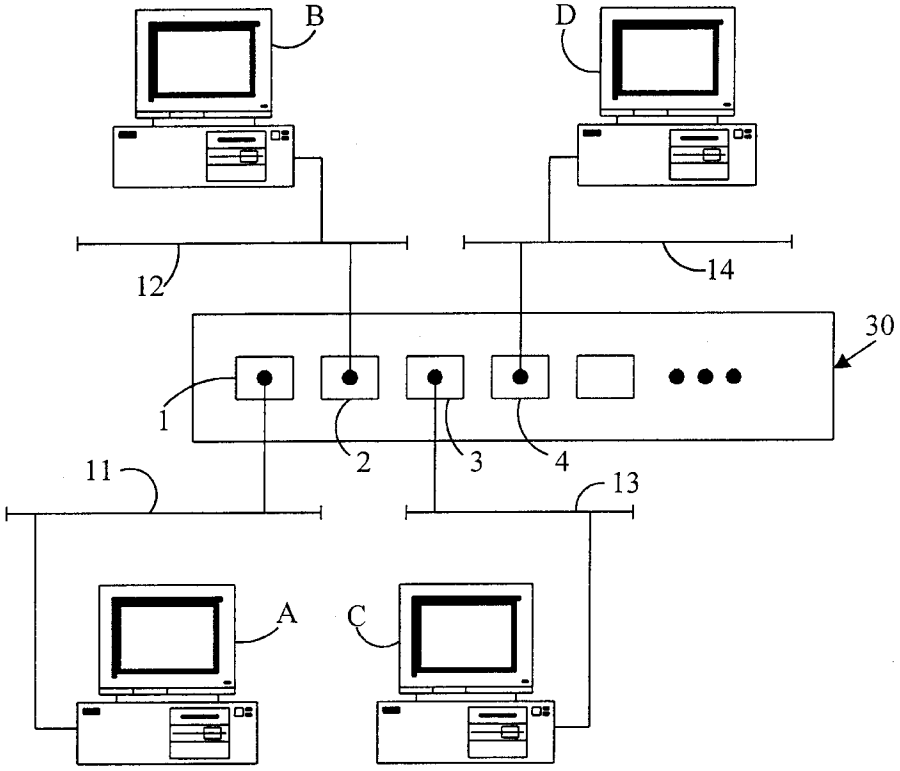
A8
B8
C8
D8

六、申請專利範圍

7.如申請專利範圍第 6 項所述之一種網路交換系統對線上封包之監控管理方法，其中該中央處理器在偵測到流經該網路交換系統之封包資料之來源位址或目的位址係該被監控之節點時，將立即依該轉送設定表內使用者所設定之參數值，進行下列監控及轉送處理：

判斷該轉送設定表中該狀態欄位內所設定之參數值，俾依該參數對所接收之封包資料，進行過濾或收集處理，並於完成該等處理後，依該轉送設定表中該連接埠欄位內所設定之連接埠，將封包資料透過該連接埠轉送到其目的位址。

圖式

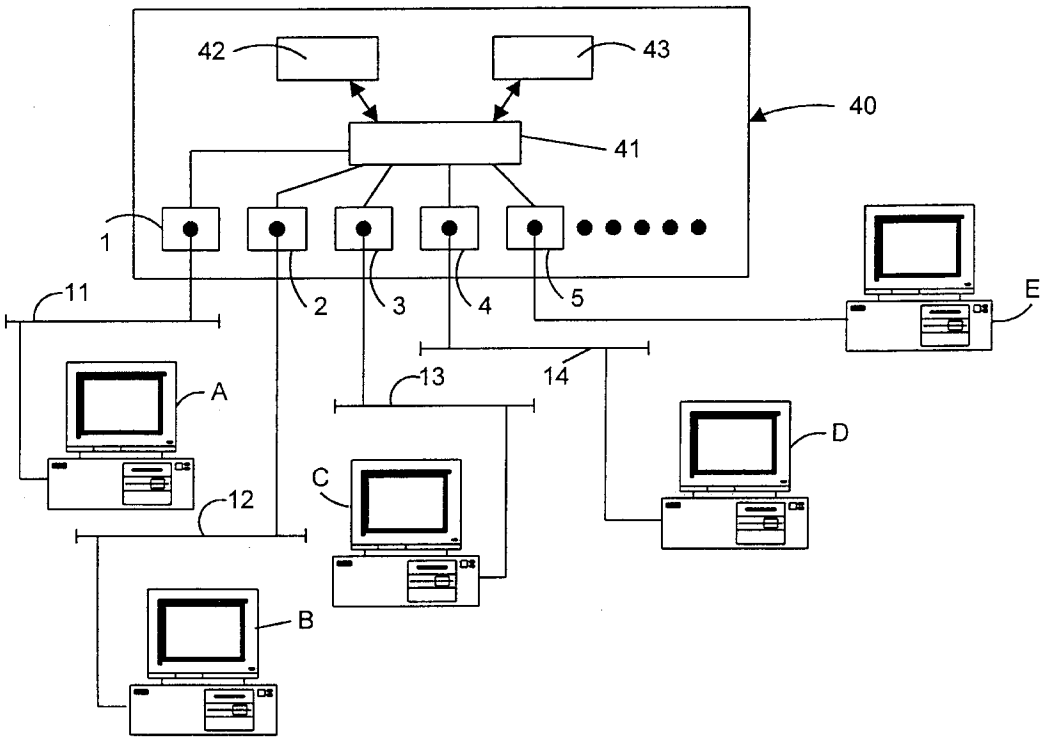


第 1 圖

節點	連接埠
A	1
B	2
C	3
D	4
. . .	. . .

31

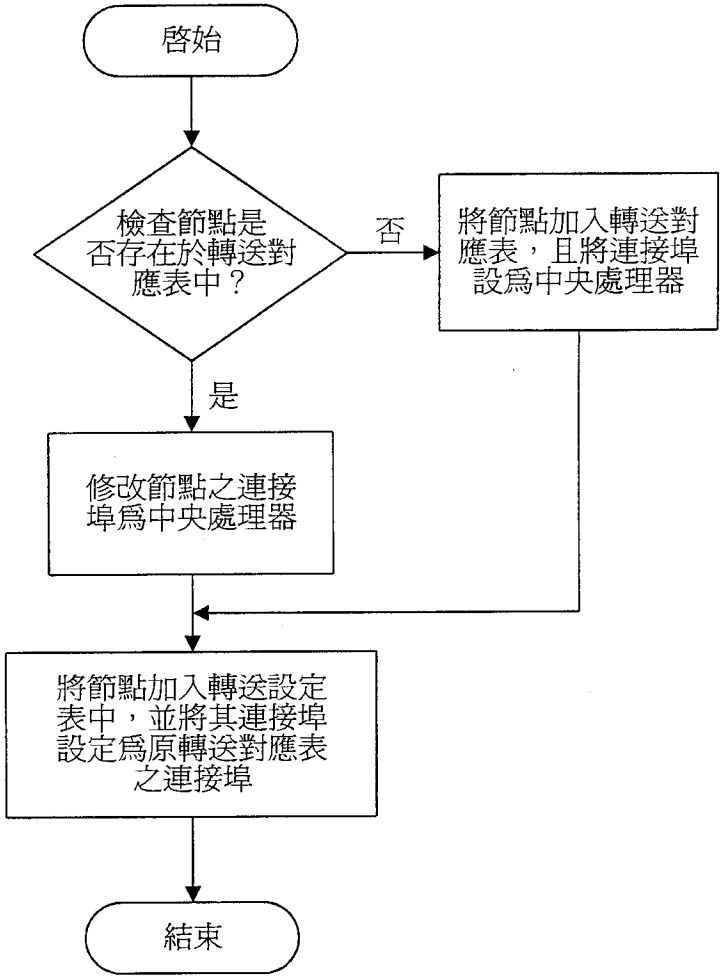
第 2 圖



第 3 圖

節點	連接埠	擷取連接埠	狀態	觸發
⋮	⋮	⋮	⋮	⋮

第 4 圖


啓始
檢查節點是否存在於轉送對應表中？
否
將節點加入轉送對應表，且將連接埠設爲中央處理器
是
修改節點之連接埠爲中央處理器
將節點加入轉送設定表中，並將其連接埠設定爲原轉送對應表之連接埠
結束

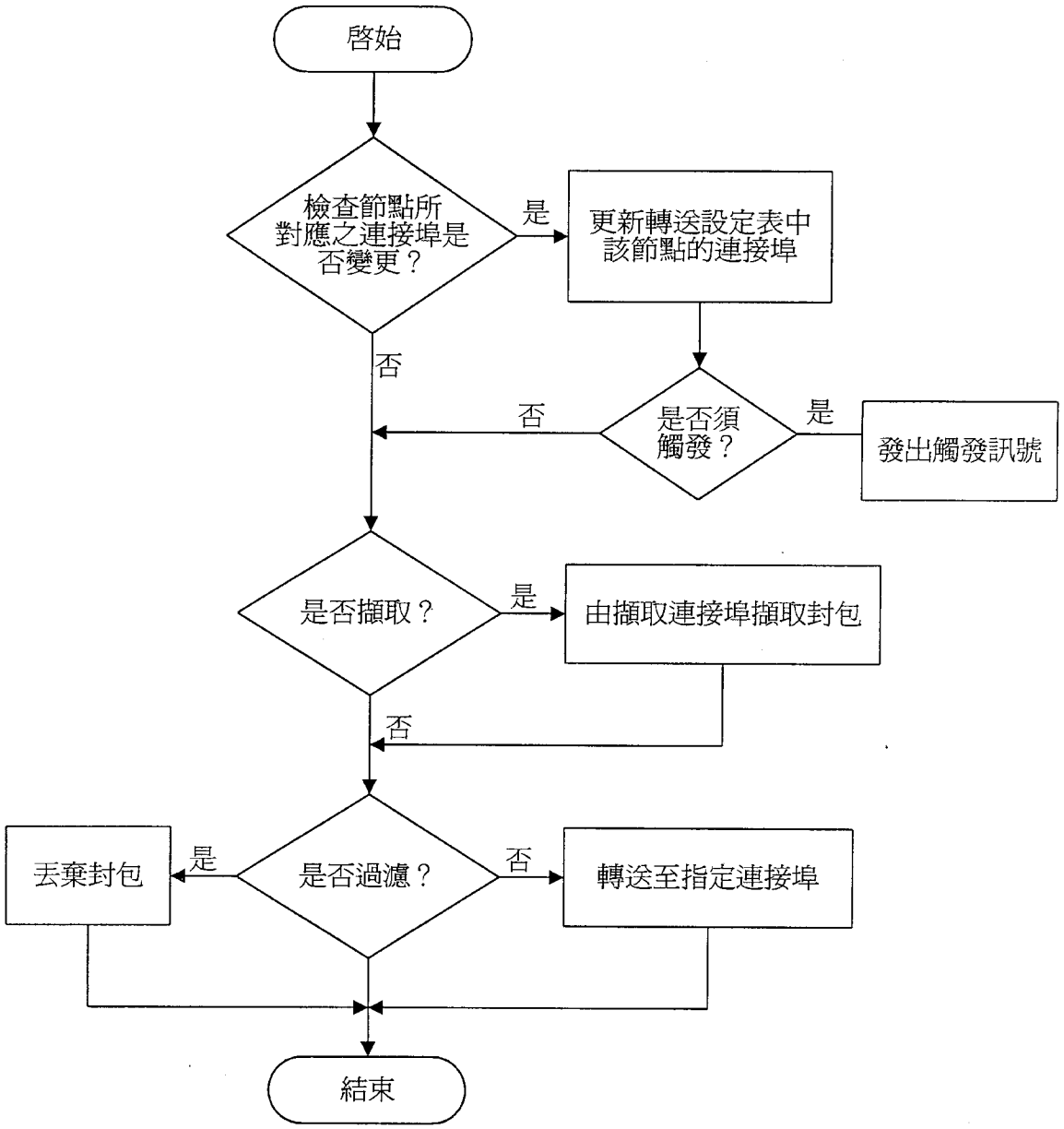
第 5 圖

節點	連接埠
A	CPU
⋮	⋮

第 6 圖

節點	連接埠	擷取連接埠	狀態	觸發
A	1	5	3	X
⋮	⋮	⋮	⋮	⋮

第 7 圖


啓始
檢查節點所對應之連接埠是否變更？
是
更新轉送設定表中該節點的連接埠
否
是否須觸發？
是
發出觸發訊號
否
是否擷取？
是
由擷取連接埠擷取封包
否
丟棄封包
是
是否過濾？
否
轉送至指定連接埠
結束

第 8 圖

¥»µo©ú«Y¤@ºØºô¸ô¥æ´«¨t²Î(Switching System)¹ï½u¤W«Ê¥]¤§ºÊ±±ºÞ²z¤è ªk¡A¸Ó¤èªk¥D-n«Y¥O¤@ºô¸ô¥æ´«¨t²Î¯à®Ú¾Ú¨Ï¥ÎªÌ³]©w¡A¨Ì¨ä¤W-ì¦³¤§¤@Âà°e¹ï À³aí(Fowarding Table)¶i¦æ-×§ï ¡A¨Ã«Ø¥ß¤@Âà°e³]©wªí(Forwarding Configuration Table)¡A-Ú¸g¹L¸Óºô¸ô¥æ´«¨t²Î¤§«Ê¥]¸ê®Æ ¡A¯à¥ý³QÂà°e (Fowarding)¨ì¸Óºô¸ô¥æ´«¨t²Î¤§¤@¤¤¥¡³B²z¾¹(CPU)¡A¦A§Q¥Î¸Ó¤¤¥¡³B²z¾¹¹ï©Ò ±ý¶i¦æºÊ±±¤§¸`ÂI¶Ç¨Ó¤§«Ê¥]¸ê®Æ¡A¨Ì¨Ï¥ÎªÌ©ó¸ÓÂà°e³]©wªí¤º¦UÄæ¦ì¤¤©Ò³]©w ¤§°Ñ¼Æ-È¡A¶i¦æ§Y®É¾Ç²ß¡BÂ^¨ú¡B¦¬¶°¡BºÊ±±¤ÎÂà°e³B²z¡C